(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 618 550 A1**

(12) EUROPEAN PATENT APPLICATION

(21) Application number : **94200897.0**

(51) Int. Cl.[5] : **G07C 9/00**

(22) Date of filing : **31.03.94**

(30) Priority : **31.03.93 NL 9300566**

(43) Date of publication of application :
05.10.94 Bulletin 94/40

(84) Designated Contracting States :
DE FR GB NL

(71) Applicant : **N.V. Nederlandsche Apparatenfabriek NEDAP**
Oude Winterswijkseweg 7
NL-7141 DE Groenlo (NL)

(72) Inventor : **van der Sar, Pieter Willem**
Zuster Meyboomlaan 33
NL-7334 DX Apeldoorn (NL)
Inventor : **Hogen Esch, Johannes Harm Lukas**
Hoge Veld 75
NL-7122 ZN Aalten (NL)

(74) Representative : **Smulders, Theodorus A.H.J., Ir. et al**
Vereenigde Octrooibureaux
Nieuwe Parklaan 97
NL-2587 BN 's-Gravenhage (NL)

(54) Access-permitting system having decentral authorizations.

(57) An access-permitting system wherein all variable information relating to the authorization of the card within the access-permitting system, such as, for instance, with regard to the entrance(s) for which the card is valid and with regard to the point of time at or the period in which the card is valid, is provided on the card.
Each time again, this information is rendered valid for a limited period of time, by means of a special card reader/writer which, unlike the other card readers belonging to the system, is connected to a central processing unit.
Also, at the same moment, all information about access already permitted can be transferred from the card wherein this information is stored to the central processing unit.
An access-permitting system according to the invention requires hardly any costly connections between the central processing unit and the decentral systems.

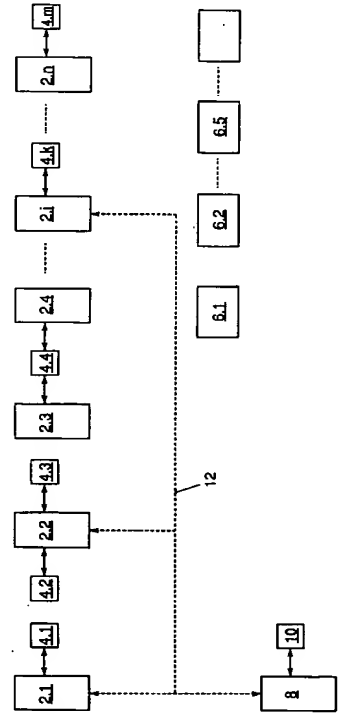

FIG. 1

EP 0 618 550 A1

The invention relates to an access-permitting system for permitting access to for instance buildings, spaces, installations, vehicles, services and/or computer systems, comprising at least one access card whereon or wherein information can be written and at least one access card reader with which information can be read from a card, which information is further processed by the system to determine whether a card can be permitted access. In such systems, known per se, cards are used, for instance in the form of magnetic cards, so-called smart cards having contacts according to the standard ISO-7816, contactless chipcards according to the standard ISO-10536, or programmable cards according to European patent number 0242906 in applicant's name, to permit access to a building, a space or, for instance, to the use of equipment. In these access-permitting systems, two main groups can be distinguished.

In the first group, the identification code or the card number of the card presented is transmitted from a card reader, arranged for instance at an entrance such as a door of a space or building, or a terminal of a computer system, to a central processing unit, whereupon it is centrally determined whether the relevant card number has access at the location where the relevant card is presented. If this is the case, a signal is subsequently transmitted from the central processing unit to the relevant entrance, for instance to open the door or to permit the terminal access to the computer system. Hence, the proper operation of these access-permitting systems depends on the lines of communication between on the one hand the different entrances and/or access card readers and on the other hand the central processing unit. The proper operation of the access-permitting system also depends on the speed at which communication takes place along these lines of communication.

In the second group of access-permitting systems, a processing unit is centrally arranged as well, also connected, via lines of communication, to card readers decentrally arranged at the entrances, the access information being present per card number in these decentrally arranged processing units. The advantage of this second group of systems is that for permitting access no communication need take place between the central processing unit and the decentral card reader, so that these systems react much more quickly and, in the event of failures, break down less quickly and not all at the same time. Consequently, a card reader may release an entrance itself after having read a card.

In the case of changes in the card file, or if the authorization of a particular card number changes, the central processing unit transmits this information via the lines of communication to all systems connected. If access is permitted by the card readers, is message hereabout is transmitted to the central processing unit. These messages need not be transmitted immediately, but may also be transmitted later, within particular limits.

Both above-mentioned groups of access-permitting systems have the drawback that a considerable infrastructure of lines of communication is necessary for transmitting messages from the central processing unit to the decentral card readers.

The object of the present invention is to provide a solution to this, wherein the above-mentioned costly lines of communication between the central and the decentral systems are required to a much lesser degree, if at all.

According to the invention, the access-permitting system is characterized in that the card comprises all relevant information relating to the access authorization of the card within the access-permitting system, so that, after reading the card, it can be determined without supplementary information whether the card can be permitted access.

The invention is based on the fact that the authorization code(s) are taken along decentrally, via the programmable access cards belonging to the system, to the different entrances in the system. Hence, in the system according to the invention, the information whether a particular card has access at a particular entrance at a particular time is contained in the card itself and need not be transmitted, via lines of communication, from a central processing unit to the decentrally arranged access card reader.

A possible drawback of such system is that in the event of loss or theft of the card, no message can be given from a central processing unit to the decentral systems in order to block the entrance for the card in question. Consequently, this would have to be reported to all individual entrances belonging to the system, for instance via a special card through which this information is conveyed to the decentral systems.

A solution to the above-mentioned problem is the introduction of a time lock or time window, of for instance one day, within which the cards are valid. In that case, the procedure can be as described below.

Each day, through a change of the information on or in the card, each card should once again be provided with all authorizations with regard to the entrances in the system, valid for that day and for that particular card. Hence, this may only take place on a system that is connected to the central processing unit. Consequently, in this manner, cards that are lost or stolen, whose authorization with regard to the entrances should be adapted in the central processing unit, are valid for one day at the most.

Another possible problem to the solution according the invention is that due to the lack of lines of communication, the information with regard to the movements of cards within the system cannot be reported to the central processing unit and hence to the system administrator. To solve this problem, it is possible to

store on or in a particular card the movements of that card as well, in addition to the authorizations of that card.

At the same time when the authorizations for a next time period are read in, the information with regard to the movements of the card within the system for the past period of time can be passed on to the central processing unit. In this manner, this information does become available in the central processing unit and hence to the system administrator, although slightly shifted in time.

The above involves that, in accordance with an advantageous embodiment of the system according to the invention, the access card reader, after reading the relevant information from the card, determines on the basis of this information whether or not access can be permitted. As a result, the system is quick and insusceptible to failures. More in particular, the relevant information of the card comprises at least one point of time or at least one period for which the access authorization of the card is valid. This may further improve the security and fraude insusceptibility of the system, because when the authorization period has ended, authorization should consciously be granted to a card holder once again. According to a very advantageous embodiment of the invention, the access authorization of the card should be rendered valid again for each new authorization period, while after the new authorization period has ended, the access authorization expires again. Consequently, the holder of the card should not be given a new card, while, however, a non-obvious positive decision is required for extending the authorization by a new period.

In particular, the system further comprises a central processing unit having a card reader/writer connected thereto, while the card can be rendered valid for a new authorization period by the central processing unit via this card reader/writer. Hence, a holder of a card wishing to extend his authorization for a new period should turn to this card reader/writer.

According to a very advantageous embodiment, the system further comprises a central processing unit to which at least one access card reader is connected, wherein, via this access card reader, the card can be rendered valid for a new authorization period by the central processing unit. This embodiment has as an advantage that an authorization for a new period can be granted to the holder of a card at an access card reader, i.e. at the moment when the holder tries to gain access with his card. In this case, it is not necessary to go to a card reader/writer especially arranged for this purpose. For instance, if it is decided before the expiration of an authorization of a card that after the expiration of the authorization the holder of the card should be given a new authorization for a new period, this can be input to the central processing unit by a system administrator, while it can also be input for which access card readers the authorization should be rendered valid. The central processing unit passes this information on to the access card readers for which the card holder presently has an authorization and/or to the access card readers for which the card holder is given an authorization for a new period. As soon as the card holder in question presents himself to one of these access card readers by giving his card to the relevant access card reader, the new authorization can be written on the card. Hence, these access card readers can also write information to a card.

To the two above-described embodiments with the authorization extension, it applies that each time, the central processing unit extends the authorization automatically, unless a system administrator blocks the automatic extension. However, it is also possible that a system administrator should each time indicate via the central processing unit whether an authorization of a card should be extended. This may for instance be entered at the central processing unit for all issued cards at the same time.

The system is in particular characterized in that the central processing unit each time extends the authorization by a new period for an indefinite time. However, it is also possible that the central processing unit each time extends the authorization period by a new period for a predetermined length of time. The length of time can for instance be 1 year, so that for this period a system administrator need not perform any direct operations. On the other hand, the automatic extension for 1 year provides an additional security of the system against errors being made, such as, for instance, the omission of inputting into the central processing unit that an employee has resigned, so that his card must no longer be automatically extended. After all, after one year the automatic extension of the authorization by, for instance, an authorization period of one day, expires.

According to a very advantageous embodiment of the invention, at the moment when access is permitted after the card has been read by an access card reader, information about the relevant entrance, which information optionally includes the point of time at which the access was permitted, is written on or in the card, this information being read out by the central processing unit when the period of validity of the card is being extended. Hence, reading out this information may take place both at the centrally arranged card reader/writer and at an access card reader connected to the central processing unit.

According to a preferred embodiment of the invention, in the event of for instance loss or theft of a card, the authorization information of this card is blocked in the central processing unit, so that the authorization of a card cannot be rendered valid again and the card, at the end of an expiring authorization period, loses its validity. Consequently, a holder who

is no longer in the possession of his card may turn to the system administrator, who will subsequently block the authorization extension in the central processing unit. Upon expiration of the authorization period, for instance, an authorization will not be automatically extended. A stolen card will then lose its validity one day (length of time of authorization period) after the theft has been reported to the system administrator.

If authorizations are not automatically extended, the blocking of an authorization may imply that simply no new authorization will be granted as described above.

If after expiration of the authorization the finder of the card has the card read out by the card reader/writer or by an access card reader connected to the central processing unit, the authorization of the card will not be extended.

Preferably, the access authorization of the card is valid for at least one predetermined entrance at which an access card reader is arranged. This makes it possible to permit card holders access only to, for instance, specific spaces of a building or specific parts of a computer system. For this purpose, the system may be provided with a plurality of access card readers, the information on the card comprising an identity code of at least one access card reader for which access can be permitted to the card in question. Accordingly, an access card reader compares, among other things, whether an identity code read out from a card corresponds to its own identity code. If this proves to be the case, and, moreover, the authorization for the relevant period is valid, access may be permitted.

Preferably, the information on the card comprises an identity code of the card. This identity code can be read out by the central processing unit in one of the above-mentioned manners to decide whether the authorization of the relevant card can be extended.

The invention will presently be further explained with reference to the accompanying drawing, wherein Fig. 1 shows two possible embodiments of an access-permitting system according to the invention.

In Fig. 1, an exemplary embodiment of an access-permitting system according to the invention is provided with a reference numeral 1. The system comprises n access card readers 2.i (i=1,2,...n), n representing a natural number greater than or equal to 1. Each access card reader 2.i is connected to at least one entrance 4.k (k=1,2,...m), m being a natural number greater than or equal to 1. In this example, access card reader 2.2 is connected to two entrances 4.2, 4.3, while entrances 2.3 and 2.4 comprise a common access card reader 4.4. The other entrances each comprise an access card reader. In this example, an entrance 4.i may be a door of a building, space, installation, a vehicle and/or any other product for which access can be permitted or refused. However, an entrance may also be, for instance, a terminal of a computer, computer network and/or any other type of computer system. The system further comprises a plurality of access cards 6.j (j=1,2,...). The number of access cards is not fixed and may vary in time. In addition, the system comprises a central processing unit 8 having connected thereto a card reader/writer 10. The access cards 6.j may for instance be magnetic cards, smart cards, contactless chipcards, programmable cards or any other type of cards on which information can be stored to be subsequently read out again. Each card 6.j comprises all relevant information on the basis of which it can be determined whether the card in question has a valid authorization for gaining access to a specific entrance 4.k. In this example, the information in question comprises a code indicating for which entrances 2.i authorization has been granted and a period for which this authorization is valid. Preferably, this authorization period is equal for each entrance 4.k registered on a card. However, it is also possible that on a card for different entrances 4.k different periods are registered for which the authorization is valid. In addition, in this example, the information on the card 6.j comprises a unique card number as identification code of the card in question.

The operation of the system 1 is as follows. A card holder of card 6.j wishing to gain access to entrance 4.k goes to a corresponding access card reader 2.i, i.e. an access card reader coupled to an entrance 4.k, and inserts his card into a slot, intended for this purpose, of the access card reader 2.i. This card reader 2.i reads from the card the entrances 4.k for which the card is authorized and the corresponding period(s) for which the card is authorized. On the basis of this information, the access card reader 2.i in question is directly capable of determining whether for the entrance 4.k in question access can be permitted to the card or, rather, the holder of the card. Hence, this does not require information from the central processing unit 8. Consequently, in this example, the central processing unit 8 is not connected to any of the access card readers 2.i. If the card has no authorization for the relevant entrance, the entrance is not released. If the period for which an authorization is valid has meanwhile expired, no access is permitted either. Obviously, for this purpose, each access card reader comprises a real-time clock. If these two conditions have indeed been met, the relevant access card reader 2.i will control the entrance 4.k in such a manner that it is released to the card holder. If a card holder presents himself to access card reader 2.2, in this example, he will have to key in, on a keyboard of this access card reader, for which of the two entrances 4.2 or 4.3 access is requested.

If an access card reader 2.i gives access to an entrance 4.k, this is registered on the relevant card by the access card reader. In this example, an identity code belonging to the relevant entrance and the point of time at which the access was given are registered

on the card.

The period for which an authorization of a card is valid will each time have to be extended after expiration thereof. If no extension of the authorization period takes place, the card will lose its validity within the system 1. To extend or renew the authorization period, a card holder should turn with his card to the card reader/writer 10. The card is inserted into the card reader/writer and the central processing unit subsequently reads the identity, i.e. the unique consecutive number of the card, via the card reader/writer 10. If all proceeds normally, the central processing unit 8 will write to the card an authorization for a new period for specific entrances 4.k via the card reader/writer 10. In general, this will mean an extension of an authorization for a specific entrance. As this authorization has again only a limited period of validity, the authorization for a specific entrance should each time be extended for a new period. Such a period may for instance be 1 day, so that an optimally safe system 1 is obtained.

If so desired, extension may also take place when the old authorization has already expired, for instance because the card holder was on a holiday. In particular, for each card a system administrator may enter into the central processing unit whether an authorization can be renewed when the old authorization for a specific entrance has already expired, while it may also be indicated for which period an authorization is extended each time. This means that for instance for one year, an authorization is each time extended by one day. Of course, this can also be programmed in such a manner that an authorization is each time automatically extended by a new period for an indefinite period.

Consequently, in general, authorizations will prefefably be automatically extended when a card is read out by the card reader/writer 10 without a system administrator having to give a specific command for this to the central processing unit 8. For this purpose, in this example, the system administrator has entered only once into the central processing unit 8 that the authorization of the card in question can be extended by a new period each time (for an indefinite time or for a predetermined time) when the card is read out, for instance at the expiration of an authorization period, by the central processing unit 8.

In this example, a new authorization period need not connect to an old period. If, for instance, a card holder has a four-day working week, the central processing unit can be programmed in such a manner that renewal of a period by a period of one day can only take place for Monday through Thursday, while no extension is possible for Friday.

However, when a card is lost or stolen, a system administrator may program the central processing unit 8 in such a manner that it is no longer possible to extend the authorization of a card 6.j. If the card in question is for instance inserted into a slot of the card reader/writer 10, the central processing unit 8 establishes that the card 6.j does not qualify for extension, whereupon an alarm signal may automatically be activated by the central processing unit 8. It is also possible that the card reader/writer 10 seizes the card by transporting it to a place inside the card reader/writer 10 closed from the outside.

It is also possible that an authorization period for a new entrance is written to the card, for instance because the card holder has been given a new work area within a building. This may also be entered into the central processing unit beforehand by a system administrator.

When a card is presented to the card reader/writer 10, the central processing unit, the central processing unit will also read out the historical data concerning the entrances 4.i and the points of time at which access was permitted to the holder of the card. In order to relieve the information capacity of a card, this information, after having been read out, may be erased from the card.

According to a particular embodiment of the invention, some or all access card readers 2.i are connected to the central processing unit 8. In Fig. 1, these connections 12 are shown in stippling. The access card readers 2.i connected to the central processing unit 8 can be used for extending an authorization by a new period as described hereinabove in relation to the card reader/writer 10.

Claims

1. An access-permitting system for permitting access to for instance buildings, spaces, installations, vehicles, services and/or computer systems, comprising at least one access card whereon or wherein information can be written and at least one access card reader with which information can be read from a card, said information being further processed by the system to determine whether a card can be permitted access, characterized in that the card comprises all relevant information relating to the access authorization of the card within the access-permitting system, so that after reading the card it can be determined, without supplementary information, whether the card can be permitted access.

2. An access-permitting system according to claim 1, characterized in that the access card reader, after reading the relevant information from the card, determines whether or not, on the basis of said information, access can be permitted.

3. An access-permitting system according to claim 1 or 2, characterized in that the relevant informa-

tion of the card comprises at least one point of time or at least one period for which the access authorization of the card is valid.

4. An access-permitting system according to claim 3, characterized in that the access authorization of the card should be rendered valid again for each new authorization period, the access authorization expiring again after the new authorization period has ended.

5. An access-permitting system according to claim 4, characterized in that the system further comprises a central processing unit having a card reader/writer connected thereto, while the card can be rendered valid for a new authorization period by the central processing unit via said card reader/writer.

6. An access-permitting system according to claim 4, characterized in that the system further comprises a central processing unit having connected thereto at least one access card reader, while the card can be rendered valid for a new authorization period by the central processing unit via said access card reader.

7. An access-permitting system according to claim 5 or 6, characterized in that at the moment when access is permitted after the card has been read by an access card reader, information about the relevant entrance, said information optionally including the point of time at which the access was permitted, is written on or in the card, said information being read out by the central processing unit when the card is read out by the central processing unit for extending the period of validity of the card by a new authorization period.

8. An access-permitting system according to any one of claims 5-7, characterized in that for an indefinite time, the central processing unit each time extends the period of validity of a card by a new authorization period.

9. An access-permitting system according to any one of claims 5-7, characterized in that for a predetermined time, the central processing unit each time extends the period of validity of a card by a new authorization period.

10. An access-permitting system according to any one of claims 5-9, characterized in that for instance in the event of loss or theft of a card, the authorization information of said card is blocked in the central processing unit, so that the authorization of a card cannot be rendered valid again and the card loses its validity at the end of an expiring authorization period.

11. An access-permitting system according to any one of the preceding claims, characterized in that the access authorization of the card is valid for at least one predetermined entrance at which an access card reader is arranged.

12. An access-permitting system according to any one of the preceding claims, characterized in that the information on the card comprises an identity code of the card.

13. An access-permitting system according to any one of the preceding claims, characterized in that the system comprises a plurality of access card readers, the information on the card comprising an identity code of at least one access card reader for which access can be permitted to the relevant card.

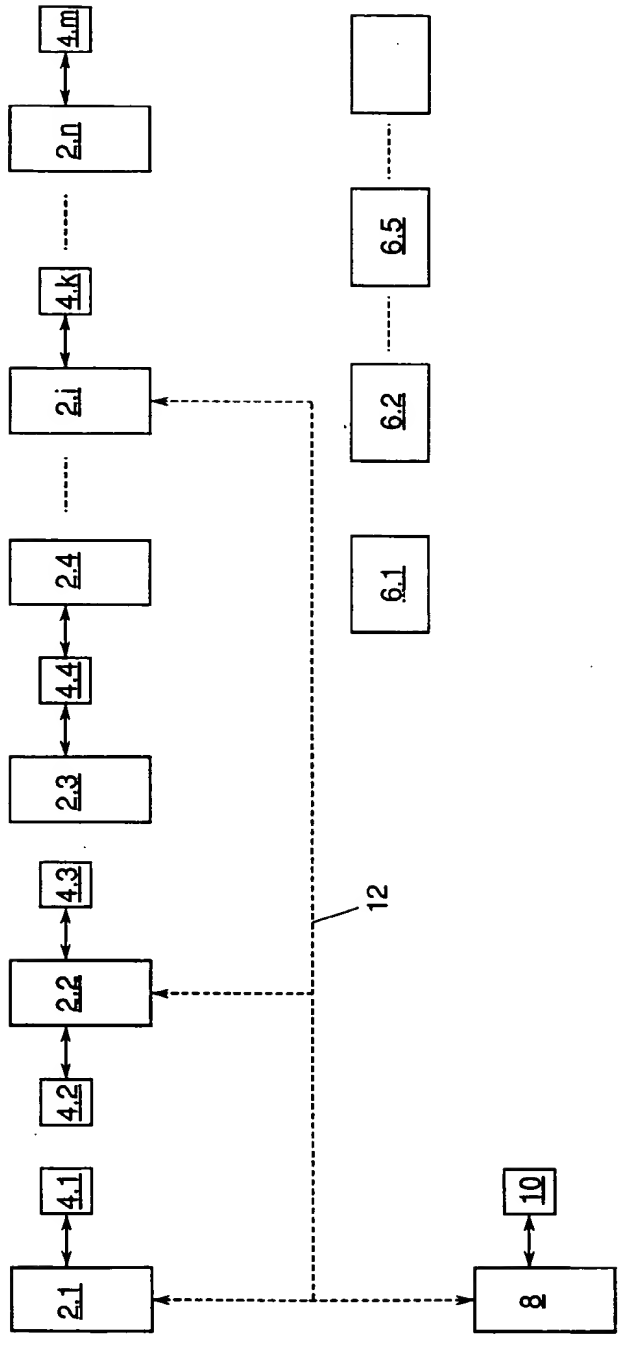

FIG. 1

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 94 20 0897

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.5)
X	WO-A-91 18169 (MEDECO SECURITY LOCKS) * page 6, line 25 - page 9, line 16 * * page 10, line 20 - page 12, line 29; claims; figures *	1-7, 11-13	G07C9/00
X	EP-A-0 122 244 (WSO CPU-SYSTEMS) * page 4, line 20 - page 13, line 16; claims; figures *	1-3,5,6, 11,12	
Y		4,7-10	
X	GB-A-2 251 266 (TRIOVING) * page 3, line 7 - page 7, line 24 * * page 10, line 25 - page 12, line 4; claims; figures *	1-5, 11-13	
Y	EP-A-0 380 377 (URBA) * column 2, line 25 - column 7, line 6; claims; figures *	4,7	
A		1,5,8,9	TECHNICAL FIELDS SEARCHED (Int.Cl.5)
Y	DE-A-35 38 733 (HOSPI DATA) * column 4, line 7 - column 6, line 16; figures *	8,9	G07C G07F E05B G07B
A		10	
Y	US-A-3 906 447 (CRAFTON) * column 8, line 22 - column 9, line 4; claims; figures *	10	
A	EP-A-0 043 270 (OMRON TATEISI) * page 4, line 2 - page 7, line 23; claims; figures *	1	
A		3-5	
A	WO-A-88 09541 (BREVATOME)		

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	8 July 1994	Meyl, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 94 20 0897

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.5)
A	WO-A-88 06826 (MARS)		

TECHNICAL FIELDS SEARCHED (Int.Cl.5)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	8 July 1994	Meyl, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)